Normative Dimensions of Paternalism and Security

LISA NELSON*

ABSTRACT

Americans are suspicious of the gathering and use of personal information by the government and the potential violations of privacy that may result. This article surmises that this level of suspicion varies depending on the types of personal information acquired and the purpose for which it is being acquired. To test this hypothesis, a survey was conducted to determine public acceptance of the use of various forms of personal information to achieve specific governmental objectives. The data revealed that the public is, in fact, willing to accept the use of personal information to achieve certain governmental objectives; however, not without limitation. Factors that affected the level of acceptance were the achievability of the policy, sensitivity of data being used, the specific governmental objective, and trust in the branch of government utilizing the data. In short, Americans must have confidence in the paternalistic judgment of the government in order to accept the gathering and use of their personal information.

I. INTRODUCTION

The events of September 11 and the war on terror pose a unique situation in which public attitudes toward the use of personal information can be examined.[1] The threat of terrorism has prompted government efforts to construct terrorist watch lists, create airline screening programs and tighten border crossings with enhanced forms of identity verification. Many of these security measures require the overt, and sometimes covert, collation of various forms of personal information from the American public. It would seem that an analysis of the law might yield a relatively simple answer to the question of whether the use of personal information for the achievement of policy objectives is appropriate. But, is there more to the story? Are there instances when the public is more willing to accept the use of information for particular governmental objectives? Does the public's

* Lisa Nelson, J.D., Ph.D., is a professor at the University of Pittsburgh, Graduate School of Public and International Affairs.

[1] As will be discussed, the phrase "personal information" is broken down into particular forms of information to assess how different forms of data might be perceived as potentially violating a sense of privacy or liberty.

confidence in the government's ability to achieve a policy objective affect attitudes about secrecy and loss of privacy? How does the public perceive the use of personal information for the purpose of fighting the war on terror? Do levels of sensitivity differ depending upon the type of personal information that is being acquired, the purpose for which it is used and the public policy benefit achieved? The answers to these questions are necessary in order to understand societal acceptance of the use of personal information to achieve policy objectives. An analysis of the law alone may not yield a complete picture.

These questions were the focus of a 100 person survey which was conducted in the summer of 2004. As a preliminary step toward understanding the complicated relationship between data sensitivity, governmental policy objectives and public perceptions of privacy and civil liberties, this survey was designed to assess public acceptance of the use of various forms of personal information to achieve specific governmental objectives. These governmental objectives included, among others: airline safety, border security, verification of tax payer information, and attempts to track down parents who were delinquent in their child support payments. The data revealed that the public was willing to accept the use of personal information to achieve particular governmental objectives with some caveats. Degrees of acceptance were affected by the confidence in the achievability of the policy directive, the sensitivity of data being used, the type of governmental objective, and confidence and trust in the particular branch of government tasked with achieving the objective. The following discussion will sketch out the nuances of public perceptions of data sensitivity, governmental objectives and levels of confidence and trust in government. This article will also discuss the implications for public tolerance of governmental secrecy.

II. PATERNALISM AND SECURITY: THE PAST, THE PRESENT AND THE FUTURE

The philosophical lens through which these questions are examined is paternalism. One might think that the reference made to paternalism is to the mantra of "big brother," which became common in the post-September 11 environment. This is not the intended reference. Instead, the use of paternalism in this discussion refers to the long standing historical and theoretical concept in democratic theory. This is not to say that paternalism is an accepted fact of democratic governance. To the contrary, the exercise of paternalistic decision making is, and has been, the subject of great debate in which

the question of societal acceptance looms large. Theorists important to our democratic tradition, such as John Stuart Mill and John Locke, looked upon paternalism as a potential threat to individual liberty. Ironically, they also considered it necessary for the preservation of liberty in society. For instance, Locke wrote:

> It may perhaps be censured as an impertinent criticism, in a discourse of this nature, to find fault with words and names that have obtained in the world; and yet possibly it may not be amiss to offer new ones when the old are apt to lead men into mistakes, as this of 'paternal power' probably has done...[2]

According to John Stewart Mill, however, the exercise of paternal power in democratic governance presents itself as a necessary evil. As Mill explains, there are times when political authority is justified in its interference with the liberty of the individual. Thus, the protection of liberty in society sometimes requires the diminution of the liberty of the individual. This is an ironic necessity in a democratic context, as Mill explains:

> ...That the only purpose for which power can be rightfully exercised over any member of a civilized community, against his will, is to prevent harm to others. His own good, either physical or moral, is not a sufficient warrant. He cannot be rightfully compelled to do or forbear because it will be better for him to do so, because it will make him happier, because, in the opinion of others, to do so would be wise, or even right. These are good reasons for remonstrating with him, or reasoning with him, or persuading him, or entreating him, but not for compelling him, or visiting him with any evil in case he do otherwise.[3]

These countervailing arguments surround the philosophical concept of paternalism and animate discussions about the use of personal information to achieve government policy objectives. In addition,

---

[2] John Locke, "The First Treatise of Government," in *Two Treatises of Government*, ed. Thomas I. Cook (New York: Hafner Publishing Company, 1947), 146.

[3] John Stuart Mill, *On Liberty, Etc.* (London: Oxford University Press, 1966), (Orig. pub. 1859), 15.

these arguments may shed light on shifting societal perceptions of the appropriateness of government policy objectives. While the ideas of John Stuart Mill and John Locke may seem far from the current policy debates, their philosophical insights on the appropriate exercise of paternalist political power are important to understanding the relationship between the use of personal information and the ongoing protection of civil liberties and privacy. Locke and Mill did not argue that the measure of appropriate paternalistic power was that of the law. Instead, the judgment of paternalist action was measured by the harm to be prevented. In the current debate involving governmental use of personal information for various policy objectives, the measure is not markedly different from that envisioned by Locke and Mill, though privacy advocates would have society believe otherwise. Determining whether harm was prevented seems to better measure societal acceptance of the use of personal information to achieve a policy objective than measuring the privacy that might be lost. Whether the public is willing to accept the use of personal information to achieve a policy objective is not solely a legal question. In fact, it seems that a normative assessment of the harm to be prevented by the policy objective drives the acceptance of personal information. Yet, it is not the mere identification of harm which drives the public's acceptance of the use of personal information, a paternalistic action. There are circumstances in which the public will accept paternalistic intervention involving the use of personal information for the achievement of a policy objective, and there are circumstances where the public will not.

III. THE PARAMETERS OF PATERNALISM

Part of understanding the acceptance and appropriateness of paternalism is coming to terms with its definition. As VanDeVeer explains, the implicit meaning attributed to paternalism is a well intentioned or benevolent motive or, in his words, the "characterization of a paternalistic act as one in which one party *interferes* with another for the sake of the other's own good."[4] Evaluation of paternalistic actions is not legal in nature. Therefore, societal acceptance hinges upon whether the action taken is ethical or morally saleable.

The difficulty in evaluating paternalism is that the actions or practices might prevent harm, promote welfare interests of subjects, or

---

[4] Donald VanDeVeer, *Paternalistic Intervention: The Moral Bounds on Benevolence* (Princeton, NJ: Princeton University Press, 1986), 17.

"blind us to the morally significant cost of such policies."[5] An ethical theory of paternalism includes a duty to protect against harm but also acknowledges an implicit moral constraint. Of course, for each different exercise of paternalistic power, it is likely that the moral constraints differ as well. In the case of the use of personal information for the achievement of policy objectives, how does the public evaluate the benevolence of motive and the achievement of a good?

Returning to Mill at this point can be helpful in laying the philosophical groundwork for understanding the substance of the survey questions. From Mill's perspective, the markers for acceptable paternalistic acts are found in the prevention of harm. The prevention of harm, however, is not so easily assessed when the use of personal information serves a range of policy objectives and, at the same time, presents a potential threat to privacy and civil liberties. This is not the easy case that Mill imagined. Mill wrote that,

> [i]f either a public officer or any one else saw a person attempting to cross a bridge which had been ascertained to be unsafe, and there were no time to warn him of his danger, they might seize him and turn him back, without any real infringement of his liberty; for liberty consists in doing what one desires, and he does not desire to fall into the river."[6]

In Mill's straightforward example, liberty is not affected when an individual is prevented from a danger that he or she would not want to choose. The danger of falling off the bridge is not in conflict with the individual's choice not to fall off the bridge. The important difference is that paternalistic power is acceptable if it prevents a harm like that of terrorism. However, unlike falling off of a bridge, an act of terrorism is random and unpredictable in nature. Thus, the liberty interests that individuals have vested in personal information might be compromised to prevent the wider ranging, often invisible danger that terrorism presents. Individuals may want to avoid a terrorist act, but they may also want to make some choices about the divulgence of personal information that run counter to the governmental interest in achieving a policy objective. The paternalistic act in this instance also becomes a potential threat to the liberty interests of individuals

---

[5] Ibid, 425.

[6] Mill, *On Liberty, Etc.*, 118.

because, unlike falling off a bridge, the choices that they want to make may be precluded in the name of preventing harm. Mill warns that this is a potential threat to an individual's liberty in these instances because the paternalistic action taken to prevent harm treads on delicate philosophical ground. Factor in secrecy, and the societal acceptance of paternalistic acts becomes even more problematic.

While paternalism presents a potential threat to liberty, the preservation of liberty does not simply require an absence of governmental paternalism. The exercise of paternalism is, in fact, necessary to preserve liberty in the face of harm. The question is: when is it appropriate to interfere with liberty to prevent harm? The calculus is strikingly simple according to Mill:

1. S's liberty to do X is infringed only if S desires to do X.
2. S does not desire to do X.
3. Therefore, S's liberty to do X is not infringed.[7]

As VanDeVeer observes, Mill's calculus for evaluating paternalistic actions is valid but presents a potential problem. "Being at liberty to perform an act is more appropriately characterized in terms of the absence of constraints or barriers to certain possible courses of action–independently of whether I do or will desire to perform them."[8]

In Mill's bridge example, no liberty interest is at stake because the choice to fall off the bridge is not one that we expect the individual to make. The liberty of choice might be compromised in a number of ways distinct from the example given by Mill. Here, VanDeVeer's insight is relevant to our discussion of acceptable paternalistic acts that make use of personal information. It is the perceived constraint on possible choices, in addition to the actual constraints, that represents the potential loss of liberty in the use of personal information to achieve a policy objective. In other words, even if a legal right is not being violated, the mere perception that it is being violated is cause enough for a lack of societal acceptance. Paternalistic actions taken to prevent terrorist threats, for instance, represent the potential existence of both actual and perceived constraints on liberty. For this reason, it is important to understand societal perceptions of constraints when determining whether paternalistic action is acceptable.

---

[7] VanDeVeer, *Paternalistic Intervention*, 30.

[8] Ibid.

In considering possible consequences for liberty, paternalistic actions may not simply impinge upon a person's liberty of action. Paternalistic actions may also entail withholding information from the public or using information in a way that is not known by the public. According to VanDeVeer, "[p]aternalism is the interference with a person's freedom of action or freedom of information, or the dissemination of misinformation, or the overriding of a person's decision not to be given information, when this is allegedly done for the good of that person."[9] Allen Buchanan uses this definition of paternalism to address the type of interference with information that might occur in a doctor-patient relationship, but the analogy applies to governmental control of information. While there may be a more direct analogy to withholding information related to terrorist threats, the government might also use different forms of information to verify an individual's identity, run a screening process or profile potential terrorists, all without the explicit knowledge of those individuals. The interference is to the individual's liberty interest through the control of information and not through a direct action. This control of information might also limit an individual's range of possible choices because it is not always clear to society how and when personal information is being used in a manner that would potentially violate a sense of autonomy or anonymity.

Paternalistic actions of this type are perhaps more problematic than those that interfere with liberty of action. Consider an analogy to the case of a physician withholding information from a patient. The justification is also framed in terms of a prevention of harm. As Buchanan states, it is "disarmingly simple."[10] The argument is as follows:

1. The physician's duty–to which she is bound by the Oath of Hippocrates–is to prevent or at least to minimize harm to her patient.
2. Giving the patient information X will do great harm to him.
3. Therefore, it is permissible for the physician to withhold information X from the patient.[11]

---

[9] Allen E. Buchanan, "Medical Paternalism," in *Paternalism*, ed. Rolf Sartorius (Minneapolis: University of Minnesota Press, 1983), 62.

[10] Ibid, 66.

[11] Ibid.

The duty to protect the patient from harm is not unlike the government's duty to prevent harm. The similarity involves the duty owed and the responsibility given to both the physician to protect the patient's interests and to the government to protect society's interests. The judgment to withhold or divulge information is made by those who control the information, whether it is a physician or the government. As Buchanan described, the judgment is not so easily evaluated:

> [W]e begin to see the tremendous weight that this paternalistic argument places on the physician's power of judgment. She must not only determine that giving the information will do harm or even that it will do great harm. She must also make a complex comparative judgment: Will withholding the information result in less harm on balance than divulging it?[12]

The dilemma of judgment is very similar for both the physician and the government. Whether it is the judgment of a doctor or a physician, the decision to control information by withholding or divulging it, is undertaken with the goal of preventing harm. Yet, in each case, a harm might occur because of the preventative action taken. Buchanan argues this point through an example of a patient with terminal cancer. "[T]he physician must not only determine that informing the patient would do great harm but that the harm would be greater on balance than whatever harm may result from withholding information."[13] The judgment entails a consideration of what the patient may or may not be able to withstand given the diagnosis, and if the patient may decide not to undergo chemotherapy because she believes that it will not benefit her. Upon consideration of these issues, the physician might decide not to tell the patient that she is going to die regardless of the treatment. Whatever the evidence for the judgment, the doctor is given a duty to assess what will be best for his or her patient. The duty of the government to achieve a policy objective, whether it is the administration of drivers' licenses or the war on terror, is somewhat similar in that a judgment must be made to withhold information or put information to use. Although harms are weighed in all of these scenarios, the risk-requiring consideration is

---

[12] Ibid.

[13] Ibid.

individual liberty will be affected by the handling of such information. The paternalistic interference with an individual's liberty interest in information is difficult because the harms are less apparent compared to the harms from interfering with an individual's liberty of action.

In these instances, the acceptance of paternalistic action to achieve a policy objective or to prevent a harm depends upon:

1. the public perceiving the action as an interference with their liberty interest;
2. whether the justification of the action is persuasive; and,
3. whether there is trust and confidence in governmental judgment.

Again, these matters are not defined by actual civil liberties and rights but, rather, by the normative perceptions of interference with liberty. For this reason, the perceptions of constraints or barriers on liberty are perhaps even more important than the violation of legal rights and liberties in evaluating and accepting paternalistic actions. Capturing societal evaluations of paternalistic actions is no easy task, especially when it turns on perceptions of constraints and barriers to liberty. However, it is a necessary starting point for understanding the complicated nature of perceptions of liberty.

IV. SOCIETAL ACCEPTANCE, DATA SENSITIVITY AND THE POSSIBLE IMPLICATIONS FOR GOVERNMENTAL SECRECY

The findings discussed below provide insight into the factors which affect the normative acceptance of paternalistic actions, while providing an understanding of when a liberty interest in privacy may be compromised by paternalistic action. The purpose of the survey was to gauge societal perceptions of data sensitivity when that data was to be used for particular policy objectives. A liberty interest in privacy is much more than its legal dimensions, and thus, understanding the acceptance of the use of personal information and the liberty interest in privacy at stake is a normative endeavor. These dimensions, the liberty interest in privacy and the evaluation of the stated policy objectives, are framed by the concept of paternalism and the terms under which it is acceptable to a polity.

The responses from the survey were the result of a random digit dial telephone interview with one hundred respondents. The respondents were almost two-thirds female (36% male and 64% female), ranging in ages from 18 to 89. The large majority of these respondents described themselves as white (85%). The second largest

group represented was black or African-American (8%). Additionally, 3% were Hispanic, and 4% were Asian or Pacific-Islander. Almost half (48%) of the respondents had a bachelor's degree or higher, and 28% of respondents had more than a four-year college degree. Fifty-one percent of respondents had a two-year degree or some four-year college education or less, and 4% of the respondents did not have a high school degree. Politically, 32% of the respondents reported being Republican, while 35% reported being Democrat. Another 13% of respondents identified with another party, and the remaining 20% did not affiliate themselves with any political party.

As part of the survey, some general questions regarding perceptions of risk were posed. These questions on perceptions of risk provide a context for understanding the type of paternalistic actions that might be acceptably taken to achieve particular policy objectives. The chance of another terrorist attack was probable in the minds of many of the respondents.

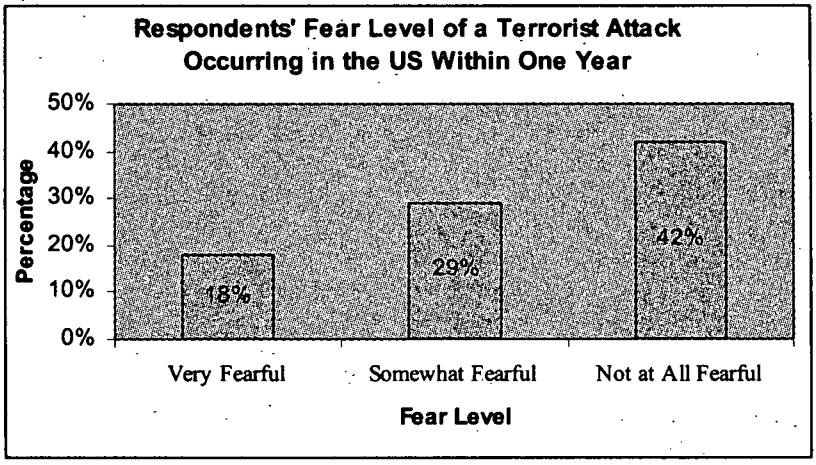

Figure 1: Respondents' Fear Level of a Terrorist Attack Occurring in the US Within One Year

More than half of the respondents (57%) were at least somewhat fearful of another terrorist attack in the U.S. in the next year, while 42% were not at all fearful. Many respondents (81%) believed that there was a high chance of another major terrorist attack in the U.S. In fact, those who indicated that they were more fearful were significantly more likely to favor the use of the following personal information as an identity check when boarding a plane than those

who were less fearful: (1) name (t = -2.166; p = .033), (2) address (t = -2.238; p = .027), (3) Social Security Number (t = -2.513; p = .014), and (4) credit card number (t = -2.719; p = .008).[14] Perceptions of risks are likely to affect the acceptance of paternalistic action. Yet, it is not only the harm of terrorism that defines a potential risk. Respondents were also concerned about the increased usage of personal information by the government. This risk, although quite different from that of fighting terror, would also affect the societal acceptance of paternalistic action taken with the usage of personal information.

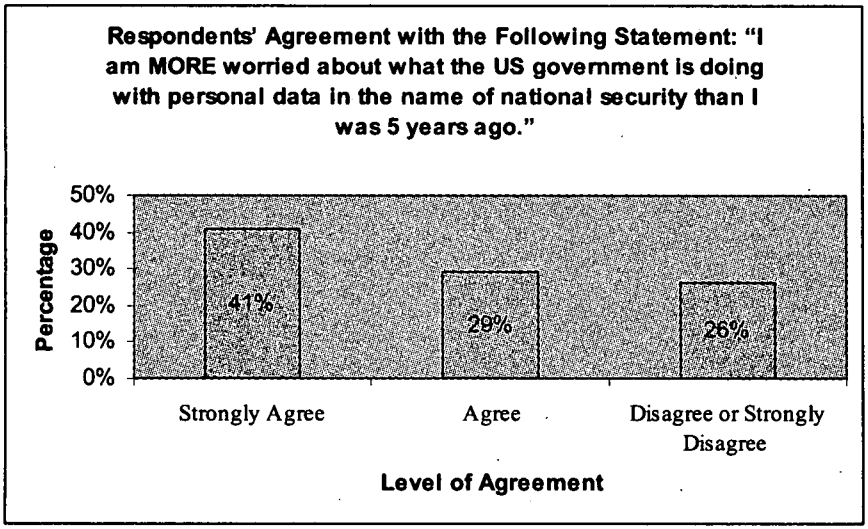

Figure 2: Respondents' Agreement with the Following Statement: "I am MORE worried about what the US government is doing with personal data in the name of national security than I was 5 years ago."

While the war on terror was one context in which societal perception of paternalistic action to achieve a policy goal was gauged, it was not the only one. As discussed above, paternalist action is quite commonplace in a democratic context, as is the use of personal information for governmental objectives. The survey began by

[14] The 't' is the value that emerges from the test, and it is checked against a probability table. The 'p' refers to probability. If the probability is less than .05, the difference is significant at the .05 level. If the probability is below .05, there is a significant result.

informing respondents that certain forms of personal data were already being used for particular public policy purposes. For instance, respondents were informed that the Internal Revenue Service (IRS) uses personal information such as name, address, date of birth, and social security number, to make sure that people have filled out their tax returns accurately, and that the IRS does this by matching information from the tax returns with information from other organizations regarding payments and other kinds of transactions. This was done to establish current acceptance of the use of personal information to achieve policy objectives and to better understand acceptance of paternalistic actions in general.

The survey found that 70% of respondents reported being aware of this use of personal information, establishing a baseline for knowledge of information usage. The survey then determined how supportive individuals were of using such data for this public policy purpose, finding that 70% of respondents were in favor of using personal information in this way. To gauge the effect that data sensitivity would have on the perception that this use of personal information would create a constraint on their liberty interest in privacy, the survey queried respondents on whether they would support the use of additional information. Sixty-two percent of respondents favored using driver's license numbers for this purpose. Yet, on the question of also using credit card information, only 23% were in favor.

The tipping point on societal acceptance of paternalistic action taken under the auspices of the IRS turned on the type of information that was being used and the purposes for which it was designated. The use of credit card information was deemed unnecessary for the achievement of the administrative purposes of the IRS and an infringement on the respondents' liberty interest in privacy. The acceptance of using particular forms of personal information seemed driven by the type of information used and the perception that certain information was not necessary to achieve the purpose stated by the IRS. Personal information, such as driver's license number, social security number, name, address and date of birth, seemed to be viewed as personal information which was characteristically used to achieve administrative purposes or policy objectives, while credit card information was viewed as an illegitimate or unnecessary piece of personal information.

achieved? Like confidence in the judgment of a physician, acceptance of paternalistic action might be affected by the existence of safeguards that protect against erroneous judgment. For instance, respondents were asked whether their willingness to provide personal information would be affected favorably if DHS were to protect their information according to various safeguards.

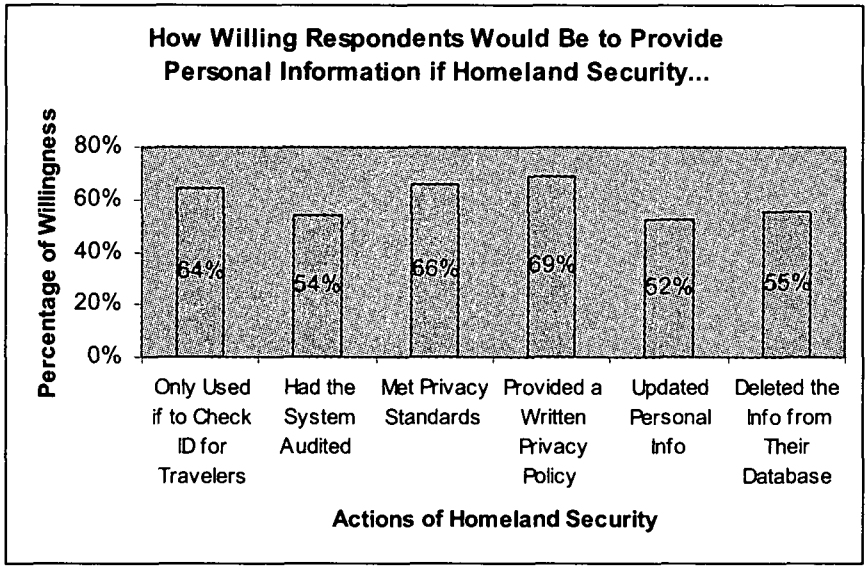

Figure 8: Respondents' Confidence Level in Homeland Security's Use and Protection of Personal Information

All of the safeguards mentioned in the graph above are ones which provide a substantiation of the type of judgment exercised. It seems that confidence in the soundness of the judgment may be more important than ensuring openness in the evaluation of paternalistic use of personal information to achieve governmental objectives. This finding seems consistent with other historical instances when societal acceptance of paternalistic action turned on the evaluation of the judgment being made by the government and not on the requirement that all of the information be available to those for whom the decision was made.

The public's acceptance of secrecy may be better understood by coming to terms with the acceptance of paternalistic judgment in representative government and the perception that the sanctity of judgment must be ensured with safeguards. Throughout history, the

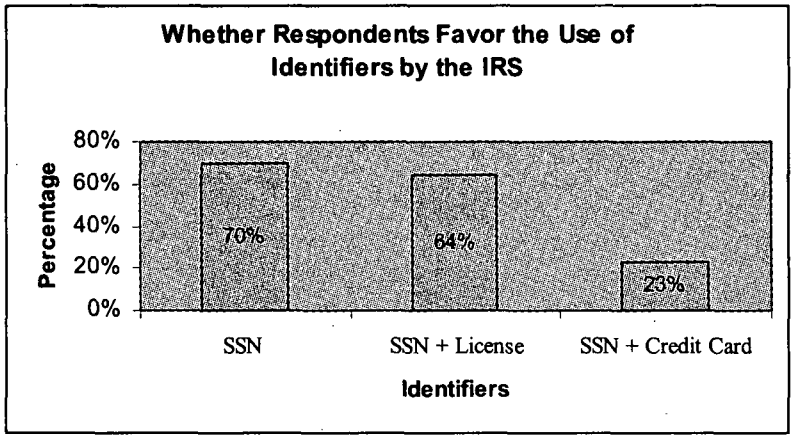

Figure 3: Whether Respondents Favor the Use of Identifiers by the IRS

Respondents were then queried about the use of personal information by the Department of Motor Vehicles (DMV). Respondents were informed that the DMV uses a database with information about all of the drivers in the United States, including: name, address, date of birth, and social security number. The DMV uses this database to determine whether a person who is trying to obtain a driver's license in one state has ever had a license cancelled, suspended, or revoked in another state. Only 37% of respondents reported being aware of this use of their personal information for these purposes; but, when queried about acceptance, 70% of respondents were in favor of using the information in this way. Yet, when asked about the use of credit card numbers, only 18% were in favor of using this type of personal information for the administrative purposes of the DMV.

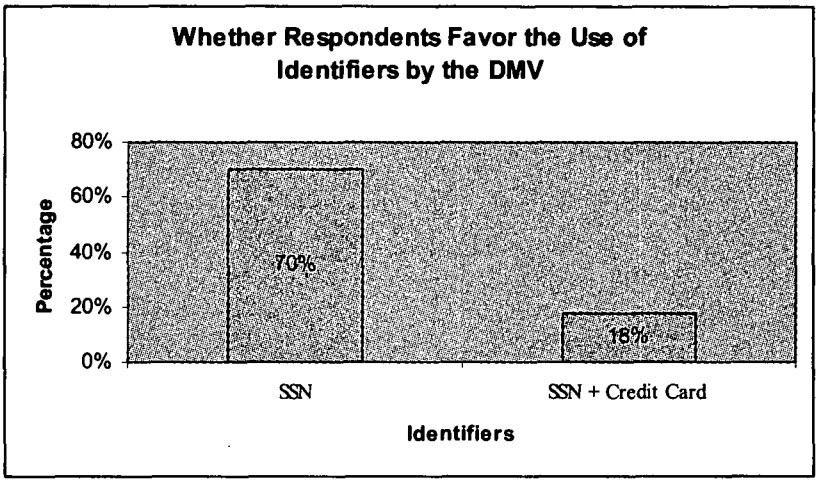

Figure 4: Whether Respondents Favor the Use of Identifiers by the DMV

These responses can be contrasted with those received when respondents were asked about their acceptance of the use of personal information for the purposes of locating delinquent parents across state lines. The respondents were informed that the database includes things like name, address, date of birth, and social security number. Ninety-one percent of respondents favored using social security numbers, 94% favored using drivers' licenses, and a relatively large percentage (43%) also favored using credit card numbers for this purpose. Some respondents even suggested taking delinquent payments from the credit card of the parent.

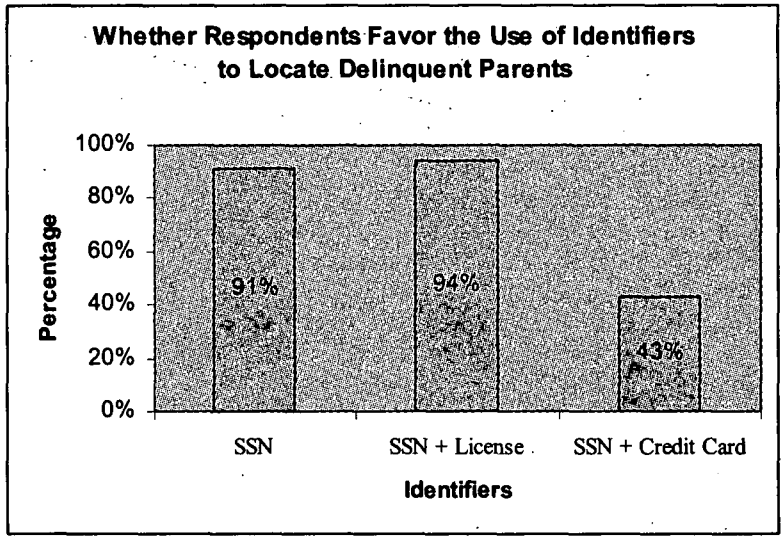

Figure 5: Whether Respondents Favor the Use of Identifiers to Locate Delinquent Parents

These baseline questions reveal some interesting dimensions of societal acceptance of paternalistic action involving personal information. Respondents were more likely to accept the governmental use of personal information, including credit cards, for the pursuit of so-called "dead-beat" dads. Although there was less acceptance of the use of credit card numbers by the DMV or IRS, respondents were generally supportive of using other pieces of personal information to fulfill the administrative mandates of each bureaucracy. What might explain the different dimensions of societal acceptance? The respondents balanced the goal of tracking down "dead-beat" dads against the potential infringement of a liberty interest in privacy. The balancing resulted in an overwhelming number of people favoring tracking down "dead-beat" dads. What defined this acceptance? The first considerations are motive behind the policy objective and the potential good to be achieved. Respondents were willing to allow the use of more sensitive personal information to achieve the policy goal, or "good," of finding delinquent parents. Indeed, in future research, it would be interesting to explore the societal dimensions of this "good" which informed the strength of this response.

The finding that respondents approved of using personal information to track down "dead-beat" dads is congruent with finding

that respondents who were accepting of the administrative goals defined by the IRS and DMV and of the use of personal information that each required. Respondents were also willing to cede information to the DMV for a database with information about all of the drivers in the United States, including name, address, date of birth, and social security number. The DMV uses the information in this database to determine whether a person who is trying to get a driver's license in one state has ever had a license cancelled, suspended, or revoked in another state. Societal acceptance was relatively high for this type of use. Recall that the second evaluation of paternalistic action is defined by control over personal information. In each of the above cases, the use of personal information was acceptable as long as it was deemed relevant to the policy goal and was viewed as achievable with the information requested. In the case of the DMV and the IRS, respondents did not view control over credit card information as necessary to achieve the respective administrative tasks, but were more willing to allow it in the case of delinquent parents.

The last evaluative prong is the perception of the societal "good" that is achieved by paternalistic actions. Respondents were more likely to support using personal information, even in the form of credit cards, when the governmental policy objective was designed to achieve what they perceived to be a "good," whether it was the identification of parents delinquent in child support payments, the verification of tax payer information, or the identification of drivers who were not in compliance with DMV requirements. The identification of parents delinquent in child support payments received the greatest support and the least concern with the divulgence of personal information. Where individuals perceived paternalistic action as necessary, they tended to accept the use of personal information, even when there was a potential loss of control over personal information. Individuals were willing to allow the use of this type of information to a greater degree when the policy goal was desirable. These initial findings indicate that the nature of the policy goal, encompassing both the motive and the good to be achieved, affects the acceptance of the use of personal information as well as the perception of the legitimacy and attainability of the objective.

The survey moved from an identification of existing uses of personal information to achieve policy objectives to some proposed uses. To this end, each survey participant was asked a set of questions about what he believed should be required for an identity check before travelers board planes. Keeping a balance between privacy, data sensitivity and a public policy purpose, the intent of these questions was to determine how individuals perceived the use of certain forms of personal data for the purpose of verifying an individual's identity

before boarding an airplane. The public policy benefit was defined as the possible reduction of terrorism. Data elements were presented to the respondents separately to gauge particular sensitivities, in light of the benefit of a potential increase in airline safety. It is important to first note that 30% of respondents do not fly on a commercial airliner in a typical year, and another 12% of the respondents reported that they fly less than once a year. Respondents were asked about their acceptance of various forms of personal information for the purposes of verifying the identity of a traveler. Most were in favor of travelers providing their names (96%), addresses (87%), dates of birth (87%) and drivers' licenses (74%), while less were in favor of providing their social security numbers (SSNs) (55%). Seventy-seven percent were opposed to travelers providing their credit card numbers.

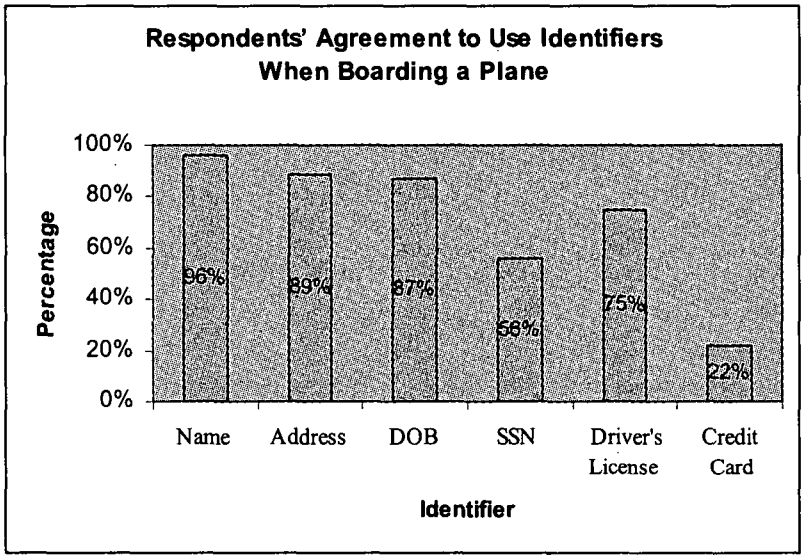

Figure 6: Respondents' Agreement to Use Identifiers When Boarding a Plane

The general acceptance of the use of name, address, date of birth and driver's license for the purposes of verifying a traveler's identity might be explained in a number of different ways. The stated policy goals of limiting terrorism and promoting airline safety affected societal acceptance of this type of personal information. Yet, the acceptance was somewhat limited. The legitimacy of using SSNs and credit card information, for instance, was perceived as falling outside

the bounds of acceptable paternalistic action of identifying travelers. This indicates that a liberty interest in privacy would be compromised in the attainment of this policy objective.

Compare these findings with the greater acceptance of all forms of personal information for the purposes of tracking down parents who were delinquent in child support payments. What drives the acceptance of one form of paternalism over the other? Is there a relationship between the type of information that is being requested and the policy objective that is used to justify paternalistic action? Clearly, some personal information is viewed as legitimate and necessary to achieving a policy objective while credit card information, for instance, is viewed as outside the range of acceptable information. This may mean that personal information created and used for a governmental purpose, like a driver's license or a social security number, is viewed with less of a liberty interest in privacy when compared to the use of credit card information co-opted for a governmental purpose. Perhaps, the origin of the information and how the information is linked to the administrative purpose for which it was created also drive the difference in acceptance. In those areas where the policy objective is novel, as is the case in the war on terror, or where the relationship between the use of personal information and the achievement of the policy objective is viewed as more tenuous or less established, some reluctance in verifying a traveler's identity may be related to a lack of established trust and confidence in the achievement of the policy goal. Does the public have greater trust and confidence in DMV and IRS usage of personal information? Does the policy goal of identifying "dead-beat" dads evoke greater confidence and trust than the identification of terrorists?

To better understand these types of questions, the survey considered societal perceptions of trust and confidence in the Department of Homeland Security (DHS) to safeguard the use of personal information. Recall the example of a physician making a judgment in the care of a patient. The evaluation of the physician's decision to withhold or divulge information did not require that the physician present all of the available information to the patient before taking paternalistic action. In fact, the judgment is one that is made solely by the physician.

The evaluation of the paternalistic act turns on the quality of the judgment, with the expectation that the information is best evaluated by the physician rather than the patient. Is the same true of the judgment exercised by the government? In the case of the doctor-patient relationship, the judgment of the physician is exercised to the stated benefit of the patient. There must be trust on behalf of the patient to accept this exercise of judgment. The same is true of action

taken by the government on behalf of society. The public view of the quality of government judgments can, in part, be measured by evaluating the level of trust and confidence that the public has in the ability of the government to use personal information responsibly. To gauge the trust and confidence that the public had in the government, respondents were asked a series of questions along these lines.

Respondents were divided on whether or not they generally trusted the United States government to protect their personal information and never misuse it. Fifty percent responded affirmatively when asked if they were in agreement with the statement, "I trust that United States government authorities protect my personal information and never misuse it." Forty-nine percent disagreed with the statement.

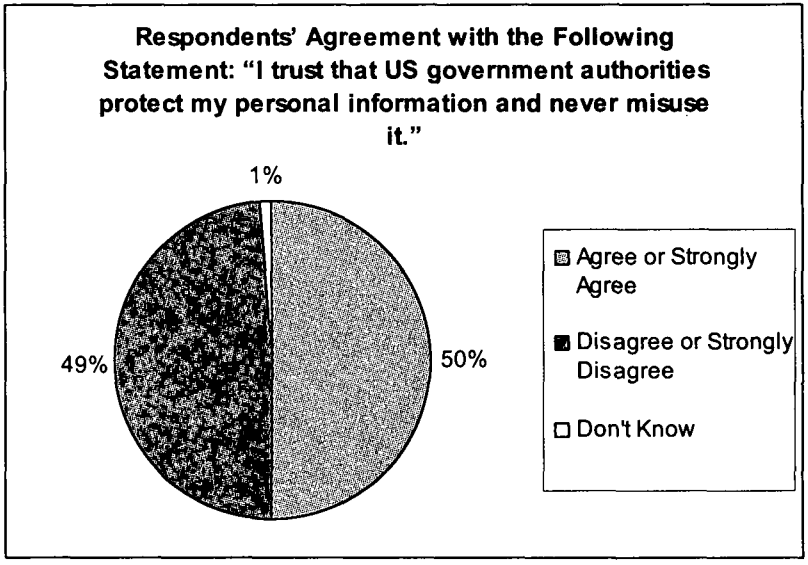

Figure 7: Respondents' Agreement with the Following Statement: "I trust that US government authorities protect my personal information and never misuse it."

On the other hand, most respondents believed that requiring personal information for identity verification would be somewhat effective (77%) or very effective (18%) in actually reducing the risk of terrorism. One-fifth (20%) believed it would not be effective at all. The acceptance of the use of personal information by the government to achieve stated policy objectives is driven by countervailing sentiments. On the one hand, a majority of respondents believed that

the use of personal information for identity verification would be somewhat or very effective in reducing the risk of terrorism. On the other hand, there is a lack of confidence in the protection of personal information from misuse. The existence of confidence was closely related to a respondent's willingness to provide personal information.

When queried about confidence in the newly organized DHS regarding the protection of personal information and the willingness to divulge it, there were mixed levels of confidence which affected the respondents' willingness to share personal information with DHS.

Table 1: Confidence in Homeland Security and Willingness to Provide Personal Information

Survey Question	**Confidence in Homeland Security**	**Willingness to Provide Personal Information**
How confident are you that the Dept. of Homeland Security would prevent personal information from being used for anything other than what it says it would be used for, that is, to check the identity of travelers?	64%	67%
How confident are you that the Dept. of Homeland Security would prevent personal information from being used for anything other than checking the identity of travelers if the system was audited by a third party?	54%	62%
How confident are you that the Dept. of Homeland Security would protect personal information in accordance with privacy standards?	66%	73%
How confident are you that the Dept. of Homeland Security would protect personal information in accordance with a written privacy policy that would be given to travelers when they are requested for the information?	69%	72%
In the process of verifying your identity it is possible that inconsistencies may arise, for instance if a person recently moved and had an address change. How	52%	77%

Survey Question	Confidence in Homeland Security	Willingness to Provide Personal Information
confident are you that the Dept. of Homeland Security would correct personal information within a reasonable amount of time if this happened?		
How confident are you that the Dept. of Homeland Security would delete personal information from its database after the information was used to check the identity of travelers if it said it would do this?	55%	72%

The element of confidence reveals the acceptance of paternalistic judgments made on behalf of society. Recall that the judgment of a physician to withhold information from a patient is a form of paternalism which, while potentially detrimental to the rights of the patient, is nonetheless a practice in the medical profession. Discretionary judgment is also part and parcel of our representative democracy where confidence in representatives underpins their authority to make decisions and judgments on behalf of their constituents. In both instances, the acceptance of paternalistic judgment does not turn on an appraisal of all of the evidence used as the basis of the judgment but rather, depends upon the confidence in the individual taking paternalistic action on one's behalf.

Does this finding have some bearing on societal perceptions of secrecy in the post-September 11 environment? If respondents are confident that personal information is used only for its intended purpose, they are not necessarily making their confidence dependent upon the ability to know all governmental uses of their personal information. The question, in other words, is one that does not ask about the openness of the use but rather, the judgment that DHS would exercise in handling personal information. The absence of the condition of overt or covert use is, in and of itself, revealing. Is it necessary to have the ability to evaluate the evidentiary basis of a judgment to place trust and confidence in the judgment of a physician or the government? It would appear that it is not. The perception that the judgment is valid and trustworthy seems more important than the requirement that the evidence upon which the decision was based is available for scrutiny. Yet, how is confidence gained and a willingness to abide by the paternalistic use of personal information

pursuit of internal security has made use of information gathering, both overtly and covertly. As John Jay stated in The Federalist No. 64, "[t]here are cases where the most useful intelligence may be obtained, if the persons possessing it can be relieved from apprehensions of discovery."[15] John Jay was not alone amongst the founding fathers of the Constitution. The value in withholding certain types of sensitive information, whether it was military or diplomatic intelligence, was an acceptable and necessary tenet in democratic governance.[16] The Supreme Court has also affirmed the need for secrecy throughout the history of its jurisprudence. The Court stated, "[i]t is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation."[17]

Yet, there have also been times in the history of the United States when paternalistic action was viewed with suspicion. Consider points in the history of the United States when confidence in the government's judgment has waned. "Under the guise of patriotic purpose and internal security, the Federalists enacted a program designed to cripple, if not destroy, the Jeffersonian party."[18] The Alien and Sedition Acts of 1798 are early examples of a paternalistic judgment which gradually lost public acceptance. Opposition to the most controversial of the Acts, the Alien Friends Law (allowing the President to order deportation of aliens) and the Sedition Law (making seditious libel a criminal offense)[19] grew in large part due to lack of confidence in the judgments being made and fear that there was no oversight when powers were exercised under these Acts' authority. Similarly, the "Red Scare," of which Joseph McCarthy was symbolic, was not unlike the fear of French invasion that fed the call for the Alien and Sedition Acts. With increasing international frustrations and rising tensions with the Soviet Union following the end of World War II, evidence of Communist espionage at the national level led to the

---

[15] Hamilton, Alexander, John Jay, and James Madison, *The Federalist*, ed. Henry Cabot Lodge (New York: The Knickerbocker Press, 1888), 403.

[16] Robert F. Turner, *War and the Forgotten Executive Power Clause of the Constitution: A Review Essay of John Hart Ely's War and Responsibility*, Virginia J. of International Law 34, no. 4 (1994): 903, 922.

[17] *Haig v. Agee*, 453 U.S. 280, 307 (1981) (quoting *Aptheker v. Sec'y of State*, 378 U.S. 500, 509 (1964)).

[18] James M. Smith, *Freedom's Fetters: The Alien and Sedition Laws and American Civil Liberties* (Ithaca, NY: Cornell University Press, 1956), 21.

[19] Ibid, 435-42.

movement to cleanse America of Communist influence. The combined effort of the Republicans, with the use of the House Un-American Activities Committee (HUAC), and Truman's loyalty boards led to action based on anonymous accusations, exploration of political beliefs of employees, and the gathering of evidence by investigating committees of the Federal Bureau of Investigation. "State governments followed suit with loyalty investigations of their own... while private industry and some unions adopted loyalty programs."[20] Eventually, the unsanctioned pursuit of Communists came under question as confidence began to wane in the judgments being made.

Though a more detailed comparison of these points in history with the current context is outside of the scope of this paper, it is possible to posit some explanations for societal acceptance of the use of personal information in the pursuit of governmental policy objectives and comment on possible implications for understanding societal perceptions of secrecy. It appears that societal acceptance of the use of personal information for the pursuit of policy objectives is driven by confidence in the judgment being made. The elements of the judgment include the evaluative prongs of paternalism that have been discussed, including the motive for and the posited good of the stated policy. In those instances when trust and confidence have not been established, some safeguards are needed to ensure that the judgment is in keeping with the stated policy objective. This finding might have also been true for societal acceptance, or eventual lack thereof, in the search for Communists during the Red Scare. The sense that paternalistic judgments by the government could no longer be trusted undermined societal acceptance of the policy objectives and the use of information to achieve them.

When confidence in governmental objectives or institutions is not well established, safeguards seem to assuage the public and ensure acceptance of the use of personal information to achieve policy objectives. This may explain a relative lack of confidence in current DHS policy objectives and a higher level of confidence when safeguards are in set place. These findings may indicate that it is not a matter of whether the use of personal information is covert or overt but rather, a matter of how much trust and confidence can be placed in the paternalistic action undertaken. Based upon this study, it appears that elements of paternalistic judgment are perhaps more important than

---

[20] Seth Kreimer, *Sunlight, Secrets, and Scarlet Letters: The Tension between Privacy and Disclosure in Constitutional Law*, University of Pennsylvania Law Review 140, no. 1 (1991), 16-17.

whether society has the opportunity to evaluate the evidentiary basis of the decision.